Ken Human
John Stealey

APOLLO, COLUMBIA & CHALLENGER CASE STUDIES

Introduction

- **Overview**
  - Why we're here
  - Organizational "culture", leadership and the model technical organization
  - Rules of engagement
- **Case Study Discussion**
  - Apollo 13
  - Challenger
  - Columbia
- **Conclusion**

Key Concepts

- Technical Competence versus Bureaucratic Process
- Schedule Pressure versus Safety as a Priority
- Normalization of Deviance
- Suppressing versus Encouraging Dissent
- The Role of Data in Decision Making
- Attributes of a Model Technical Organization

Apollo 13

Launched April 11, 1970

Apollo 13

- **Physical Cause**
  - Cryogenic tank heater circuit design flaw;
  - Teflon insulation damaged during pre-launch testing;
  - Bare copper wires in the tank were submerged in liquid oxygen during servicing;
  - On day 3 of mission, during cryo tank 2 stir, a spark jumped between wires of the heater circuit.

Apollo 13

- Apollo Culture

"Okay, listen up. When you leave this room, you must leave believing that this crew is coming home. I don't give a damn about the odds and I don't give a damn that we've never done anything like this before. Flight control will never lose an American in space. You've got to believe, your people have to believe, that this crew is coming home. Now let's get going."

Gene Kranz
Lead Flight Director
April 11, 1970

Challenger, STS-51L Launched January 28,1986

Challenger, STS-51L

- Physical Cause - Solid Rocket Booster Field Joint Design Deficiency
  - Cold temperature reduced ability of O-ring to seal Field Joint
  - Exhaust gas leaked from Right SRB
  - Weakened P-12 Strut failed
  - SRB rotated into External Tank
  - Structure broke apart, Orbiter rotated, exceeded structural limits

Challenger, STS-51L

- Organizational Cause
  - Lack of safety emphasis regarding doubts about the SRB joint seal
  - Launch constraint waivers at the expense of safety and not reviewed by all levels of management
  - Internal problem resolution focus rather than communicating externally
  - Contractor management overruled their own engineers to accommodate its customer

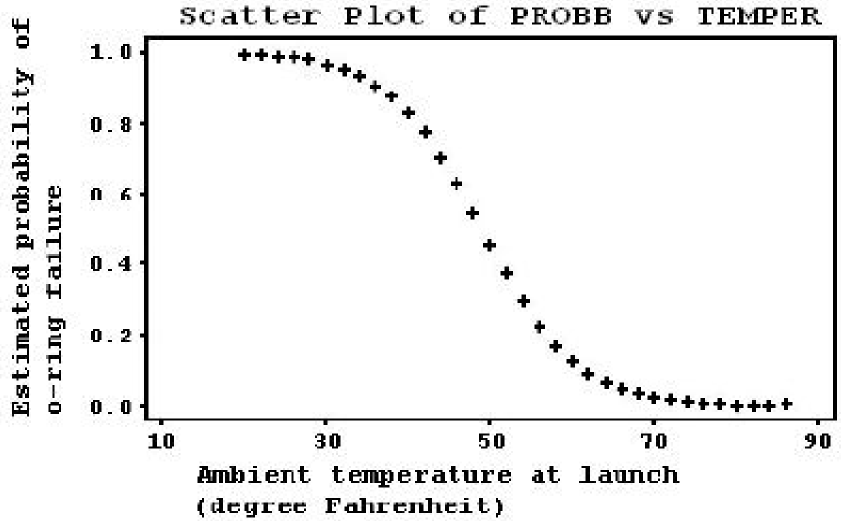
Normalization of Deviance

- When 1977 tests indicated some joint opening, contrary to joint designers' expectations, a sealing putty "fix" was added, and the anomaly was considered an "acceptable risk."
- When a 1981 launch resulted in blow-by through the putty, this anomaly was explained as a result of improperly applied putty.
- When 1984 and 1985 launches caused more leakage, this leakage had come to be expected, and acceptable.

Study Guide

Challenger Case Study

Statistical Analysis of O-ring Failure Data Available Prior to Challenger



"…with the benefit of hindsight, it can be seen that the Challenger disaster was not at all surprising, given data that were available at the time of the flight. As a result of its investigations, one of the recommendations of the commission was that a statistician be part of the ground control team from that time on."

"The Flight of the Space Shuttle Challenger," Jeffrey S. Simonoff, 1999.
http://www.stanford.edu/class/stat201/reading/challlog.pdf

Columbia, STS-107

Launched January 16, 2003:

Deorbited February 1, 2003

Columbia, STS-107

- **Physical Cause of Accident**
  - Ascent
    - Insulating foam separated from the left bipod ramp of the External Tank (81.7 seconds after launch)
    - Breached leading edge of the left wing
  - Entry
    - Superheated air penetrated, progressively melted the aluminum, weakened structure; increasing aerodynamic forces caused loss of control, failure of the wing, and breakup

Columbia, STS-107

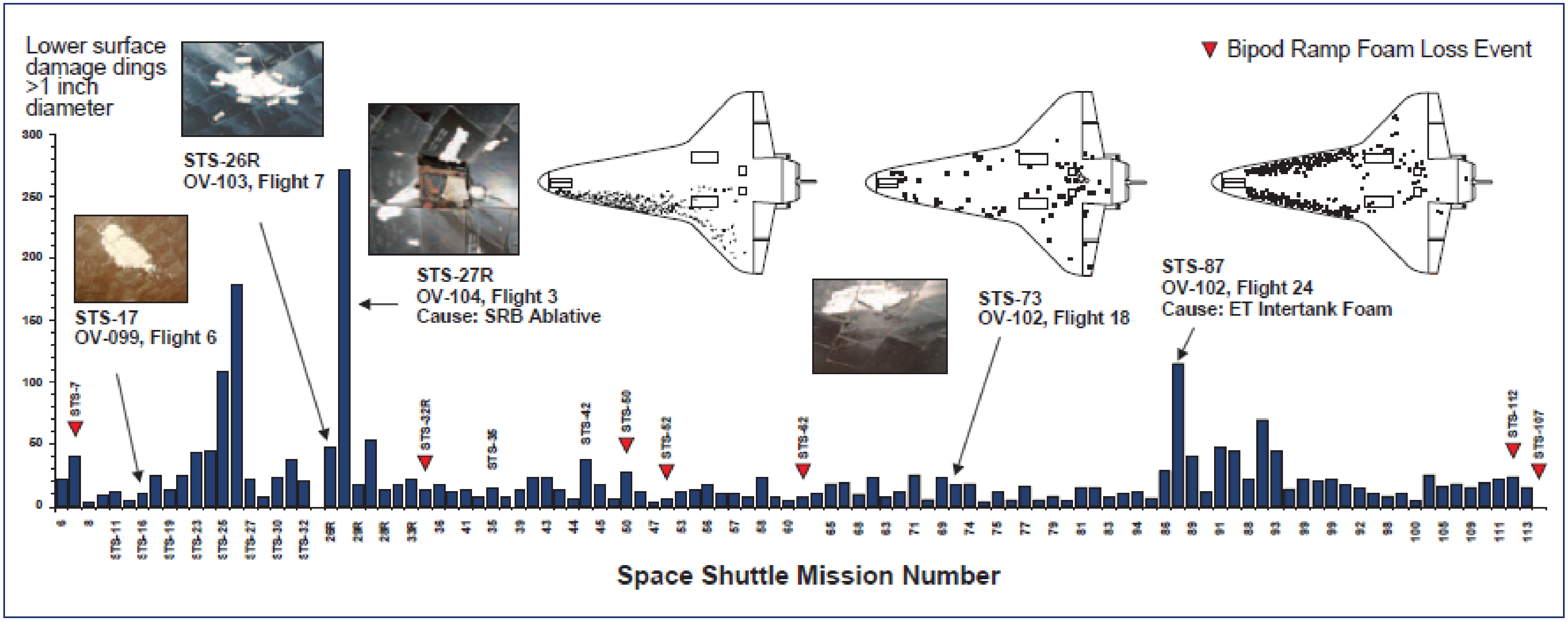


Figure 6.1-6. This chart shows the number of dings greater than one inch in diameter on the lower surface of the Orbiter after each mission from STS-6 through STS-113. Flights where the bipod ramp foam is known to have come off are marked with a red triangle.

Flights with Significant TPS Damage (14)

MISSION	DATE	COMMENTS
STS-1	April 12, 1981	Lots of debris damage. 300 tiles replaced.
STS-7	June 18, 1983	First known left bipod ramp foam shedding event.
STS-27R	December 2, 1988	Debris knocks off tile; structural damage and near burn through results.
STS-32R	January 9, 1990	Second known left bipod ramp foam event.
STS-35	December 2, 1990	First time NASA calls foam debris "safety of flight issue," and "re-use or turn-around issue."
STS-42	January 22, 1992	First mission after which the next mission (STS-45) launched without debris In-Flight Anomaly closure/resolution.
STS-45	March 24, 1992	Damage to wing RCC Panel 10-right. Unexplained Anomaly, "most likely orbital debris."
STS-50	June 25, 1992	Third known bipod ramp foam event. Hazard Report 37: an "accepted risk."
STS-52	October 22, 1992	Undetected bipod ramp foam loss (Fourth bipod event).
STS-56	April 8, 1993	Acreage tile damage (large area). Called "within experience base" and considered "in family."
STS-62	October 4, 1994	Undetected bipod ramp foam loss (Fifth bipod event).
STS-87	November 19, 1997	Damage to Orbiter Thermal Protection System spurs NASA to begin 9 flight tests to resolve foam-shedding. Foam fix ineffective. In-Flight Anomaly eventually closed after STS-101 as "accepted risk."
STS-112	October 7, 2002	Sixth known left bipod ramp foam loss. First time major debris event not assigned an In-Flight Anomaly. External Tank Project was assigned an Action. Not closed out until after STS-113 and STS-107.
STS-107	January 16, 2003	*Columbia* launch. Seventh known left bipod ramp foam loss event.

Figure 6.1-7. The Board identified 14 flights that had significant Thermal Protection System damage or major foam loss. Two of the bipod foam loss events had not been detected by NASA prior to the Columbia Accident Investigation Board requesting a review of all launch images.

Briefing Slide from STS-113 FRR

(launched November 2002)

- STS-112/ET-115 Bipod Ramp foam loss

  Missing foam on –Y Bipod Ramp - Picture

  - **Issue**
    - Foam was lost on the STS-112/ET-115 –Y bipod ramp (˜4" X 5" X 12") exposing the bipod housing SLA closeout
  - **Background**
    - ET TPS Foam loss over the life of the Shuttle Program has never been a "Safety of Flight" issue
    - More than 100 External Tanks have flown with only 3 documented instances of significant foam loss on a bipod ramp

Briefing Slide from STS-113 FRR

(launched November 2002)

- **Rationale for Flight**
  - Current bipod ramp closeout has not been changed since STS-54
  - The Orbiter has not experienced “Safety of Flight” damage from loss of foam in 112 flights (including 3 known flights with bipod ramp foam loss)
  - There have been no design / process / equipment changes over the the last 60 ETs (flights)
  - All ramp closeout work (including ET-115 and ET-116) was performed by experienced practitioners (all over 20 years experience each)
  - Ramp foam application involves craftsmanship in the use of validated application processes
  - No change in Inspection / Process control / Post application handling, etc
  - Probability of loss of ramp TPS is no higher/no lower than previous flights
  - <u>*The ET is safe to fly with no new concerns (and no added risk)*</u>

Columbia, STS-107

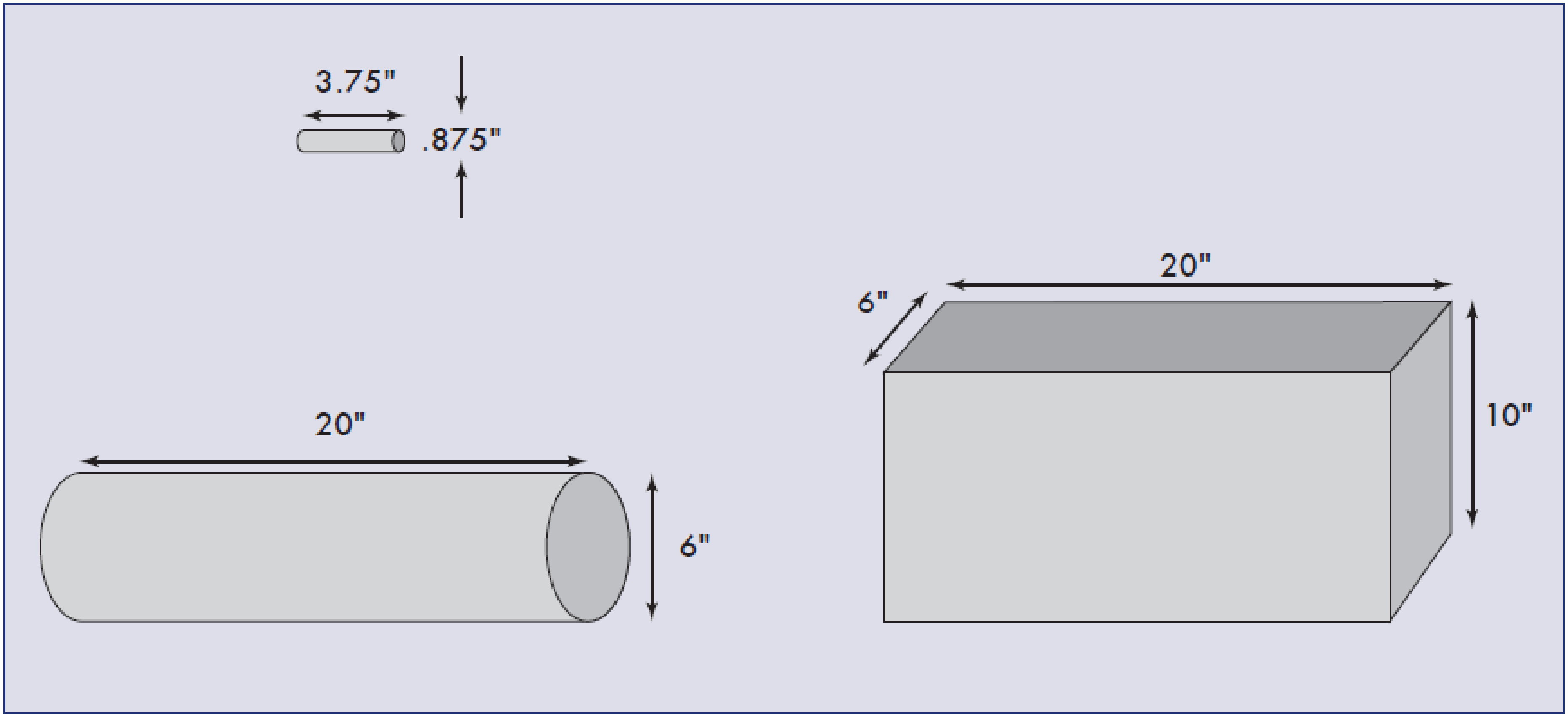


Figure 6.3-1. The small cylinder at top illustrates the size of debris Crater was intended to analyze. The larger cylinder was used for the STS-107 analysis; the block at right is the estimated size of the foam.

Review of Test Data Indicates Conservatism for Tile Penetration

- The existing SOFI on tile test data used to create Crater was reviewed along with STS-87 Southwest Research data
  - Crater over predicted penetration of tile coating significantly
    - Initial penetration to described by normal velocity
      - Varies with volume/mass of projectile (e.g., 200ft/sec for 3cu. In)
    - Significant energy is required for the softer SOFI particle to penetrate the relatively hard tile coating
      - Test results do show that it is possible at sufficient mass and velocity
    - Conversely, once tile is penetrated SOFI can cause significant damage
      - Minor variations in total energy (above penetration level) can cause significant tile damage
  - Flight condition is significantly outside of test database
    - Volume of ramp is 1920cu in vs 3 cu in for test

-----Original Message-----

From: STICH, J. S. (STEVE) (JSC-DA8) (NASA)
Sent: Thursday, January 23, 2003 11:13 PM
To: CDR; PLT
Cc: BECK, KELLY B. (JSC-DA8) (NASA); ENGELAUF, PHILIP L. (JSC-DA8) (NASA); CAIN, LEROY E. (JSC-DA8) (NASA); HANLEY, JEFFREY M. (JEFF) (JSC-DA8) (NASA); AUSTIN, BRYAN P. (JSC-DA8) (NASA)
Subject: INFO: Possible PAO Event Question

Rick and Willie,

You guys are doing a fantastic job staying on the timeline and accomplishing great science. Keep up the good work and let us know if there is anything that we can do better from an MCC/POCC stand-point.

There is one item that I would like to make you aware of for the upcoming PAO event on Blue FD 10 and for future PAO events later in the mission. This item is not even worth mentioning other than wanting to make sure that you are not surprised by it in a question from a reporter.

During ascent at approximately 80 seconds, photo analysis shows that some debris from the area of the -Y ET Bipod Attach Point came loose and subsequently impacted the orbiter left wing, in the area of transition from Chine to Main Wing, creating a shower of smaller particles. The impact appears to be totally on the lower surface and no particles are seen to traverse over the upper surface of the wing. Experts have reviewed the high speed photography and there is no concern for RCC or tile damage. We have seen this same phenomenon on several other flights and there is absolutely no concern for entry.

That is all for now. It's a pleasure working with you every day.

[MCC/POCC=Mission Control Center/Payload Operations Control Center, PAO=Public Affairs Officer, FD 10=Flight Day Ten, -Y=left, ET=External Tank]

Columbia, STS-107

Columbia, STS-107

- **Organizational Causes (Conditions)**
  - Rationalization of Danger
  - Barriers to Communication, Stifled Professional Differences of Opinion
  - Informal Chain of Command and Decision-making Outside Program Rules
  - Reliance on Past Success as a Substitute for Sound Engineering Practices (Reduced Testing)

Columbia, STS-107

- **Organizational Causes (Conditions)**
  - Ineffective Checks and Balances
  - Lack of Independent Safety Program
  - Lack of Integrated Management
  - Not a Learning Organization
  - Intense Self-imposed Schedule Pressure
  - Attempted to Realize Efficiencies under Resource Constraints
  - Fluctuating Priorities
  - Lack of an Agreed National Vision

Columbia, STS-107

- **NASA Culture at the Time of Columbia?**
  - "…if there was severe damage to the tiles, nothing could be done."

    NASA's Thermal Protection System (tile) Expert

  - "it [imaging] was no longer being pursued since even if we saw something, we couldn't do anything about it. The Program didn't want to spend the resources."

    NASA's Mission Management Team Chair

Columbia, STS-107

- **Columbia Accident Investigation Board:**
  - “Based on NASA’s history of ignoring external recommendations, or making improvements that atrophy with time, the Board has no confidence that the Space Shuttle can be safely operated for more that a few years based solely on renewed post-accident vigilance.”

NASA's Human Spaceflight Challenge

- **Highly advanced leading edge technology**
  - Tremendous energy required to accelerate 100 tons to orbital velocity
  - Difficult to manage this advanced technology
    - System is large, complex, unpredictable, cannot test everything, cannot foresee all possible environments (unknown risks)
- **High Visibility**
  - Intense media coverage and public interest
- **Organizational Complexity/Size/Diversity**
  - High number of decisions and people involved per event
  - Independent safety

Conclusion

- Can we learn from the past?
- Are we a learning organization?
- How can we improve our organization?

Back-Up Slides

Space Disasters

As of 2004, Space disasters during operations or training have killed 18 astronauts and 4 cosmonauts (5% of all people who have been in space, 2% per flight) and a much larger number of ground crew.

As of November 2004, 439 individuals have flown on space flights. Twenty two have died while in space craft: Apollo 1 (3), Soyuz 1 (1), X-15-3 (1), Soyuz 11 (3), Challenger (7), Columbia (7), totaling 18 astronauts (4.1%) and 4 cosmonauts (.9%) of all the people launched.

If Apollo 1 and X-15-3 are excluded; 4% (or 18) of the 437 have died while on a spaceflight. This excludes Gus Grissom, Ed White, Roger Chaffee, and Michael J. Adams from the killed total and Chaffee and Adams from the space flight total.

from Wikipedia

Apollo 1 (AS-204) Fire

Probable Cause

- No single ignition source conclusively identified
- Evidence of several electrical arcs found

Physical Environment

- Extremely hazardous: 100 % Oxygen, 16.7 psi, many types of combustible materials
- Deficiencies in design, manufacture, installation, rework and quality control existed in the electrical wiring
- Improper emergency procedures, no escape procedures for fire, heavy Exit Hatch (1 min. manual operation)
- Emergency fire, rescue and medical teams were not in attendance (not labeled hazardous test)

After the *Challenger* disaster, both official investigations decried the competitive pressures and economic scarcity that had politicized the space agency, asserting that goals and resources must be brought into alignment. Steps were taken to assure that this happened. But at this writing, that supportive political environment has changed. NASA is again experiencing the economic strain that prevailed at the time of the disaster. Few of the people in top NASA administrative positions exposed to the lessons of the Challenger tragedy are still there. The new leaders stress safety, but they are fighting for dollars and making budget cuts. History repeats, as economy and production are again priorities. (Vaughan, 1996: 422)

Summary

- Critical Path to U.S. Core Complete driven by Shuttle Launch
  - ➢ Program Station assessment: up to 14 days late
  - ➢ Program Shuttle assessment: up to 45 days late
- Program proactively managing schedule threats
- Most probable launch date is March 19-April 19
  - ✓ Program Target Remains 2/19/04

Figure 6.2-6. By December 2002, every bit of padding in the schedule had disappeared. Another chart from the Shuttle and Station Program Managers' briefing to the NASA Administrator summarizes the schedule dilemma.

Table 1. The Physical Cause and Organizational Cause of the Columbia accident as determined by the CAIB.

Physical Cause and Organization Cause

CAIB Report Chapter 3, p49:

The physical cause of the loss of Columbia and its crew was a breach in the Thermal Protection System on the leading edge of the left wing. The breach was initiated by a piece of insulating foam that separated from the left bipod ramp of the External Tank and struck the wing in the vicinity of the lower half of Reinforced Carbon-Carbon panel 8 at 81.9 seconds after launch. During re-entry, this breach in the Thermal Protection System allowed superheated air to penetrate the leading-edge insulation and progressively melt the aluminum structure of the left wing, resulting in a weakening of the structure until increasing aerodynamic forces caused loss of control, failure of the wing, and breakup of the Orbiter.

CAIB Report Chapter 7, p177:

The organization causes of this accident are rooted in the Space Shuttle Program's history and culture, including the original compromises that were required to gain approval for the Shuttle Program, subsequent years of resource constraints, fluctuating priorities, schedule pressure, mischaracterizations of the Shuttle as operational rather than developmental, and lack of an agreed national vision. Cultural traits and organizational practices detrimental to safety were allowed to develop, including: reliance on past success as a substitute for sound engineering practices (such as testing to understand why systems were not performing in accordance with requirements/specifications); organizational barriers that prevented effective communication of critical safety information and stifled professional differences of opinion; lack of integrated management across program elements; and the evolution of an information chain of command and decision-making processes that operated outside the organization's rules.

By time of STS-107 Foam Loss was Regarded as "In-Family"

DEFINITIONS

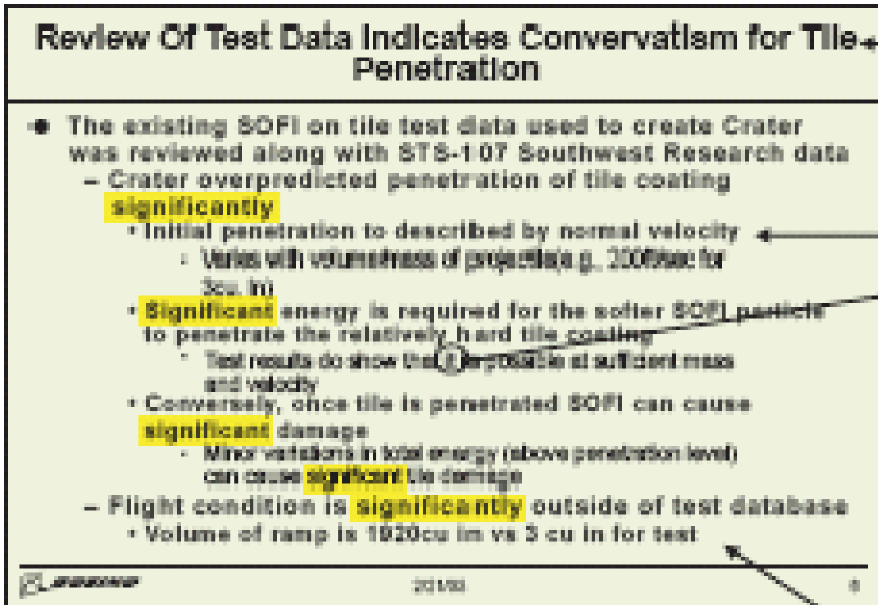
In Family: A reportable problem that was previously experienced, analyzed, and understood. Out of limits performance or discrepancies that have been previously experienced may be considered as in-family when specifically approved by the Space Shuttle Program or design project.[8]

Out of Family: Operation or performance outside the expected performance range for a given parameter or which has not previously been experienced.[9]

Accepted Risk: The threat associated with a specific circumstance is known and understood, cannot be completely eliminated, and the circumstance(s) producing that threat is considered unlikely to reoccur. Hence, the circumstance is fully known and is considered a tolerable threat to the conduct of a Shuttle mission.

No Safety-of-Flight-Issue: The threat associated with a specific circumstance is known and understood and does not pose a threat to the crew and/or vehicle.

Poor Communication via Charts



Review Of Test Data Indicates Convervatism for Tile Penetration

- The existing SOFI on tile test data used to create Crater was reviewed along with STS-107 Southwest Research data
  - Crater overpredicted penetration of tile coating significantly
    - Initial penetration to described by normal velocity
      - Varies with volume/mass of projectile(e.g., 200ft/sec for 3cu. in)
    - Significant energy is required for the softer SOFI particle to penetrate the relatively hard tile coating
      - Test results do show that it is possible at sufficient mass and velocity
    - Conversely, once tile is penetrated SOFI can cause significant damage
      - Minor variations in total energy (above penetration level) can cause significant tile damage
  - Flight condition is significantly outside of test database
    - Volume of ramp is 1920cu in vs 3 cu in for test

The vaguely quantitative words "significant" and "significantly" are used 5 times on this slide, with *de facto* meanings ranging from "detectable in largely irrelevant calibration case study" to "an amount of damage so that everyone dies" to "a difference of 640-fold." None of these 5 usages appears to refer to the technical meaning of "statistical significance."

The low resolution of PowerPoint slides promotes the use of compressed phrases like "Tile Penetration." As is the case here, such phrases may well be ambiguous. (The low resolution and large font generate 3 typographic orphans, lonely words dangling on a seperate line.)

This vague pronoun reference "it" alludes to damage *to the protective tiles,* which caused the destruction of the Columbia. The slide weakens important material with ambiguous language (sentence fragments, passive voice, multiple meanings of "significant"). The 3 reports were created by engineers for high-level NASA officials who were deciding whether the threat of wing damage required further investigation before the Columbia attempted return. The officials were satisfied that the reports indicated that the Columbia was not in danger, and no attempts to further examine the threat were made. The slides were part of an oral presentation and also were circulated as e-mail attachments.

In this slide the same unit of measure for volume (cubic inches) is shown a different way every time

3cu. in   1920cu. in   3 cu. in

rather than in clear and tidy exponential form 1920 in³. Perhaps the available font cannot show exponents. Shakiness in units of measurement provokes concern. Slides that use hierarchical bullet-outlines here do not handle statistical data and scientific notation gracefully. If PowerPoint is a corporate-mandated format for all engineering reports, then some competent scientific typography (rather than the PP market-pitch style) is essential. In this slide, the typography is so choppy and clunky that it impedes understanding.

High Reliability Organizations

- Unexpected Events
  - High Reliability Organizations find significant meaning in <u>Weak Signals</u>
    - They notice unexpected events – more, sooner, smaller
    - They concentrate more fully on the discrepancy, meaning, and resolution
    - “Don’t give weak response to Weak Signals”

Intuition

Significance of Intuition

- Intuition is a powerful internal resource and a <u>gift</u> that humans have
  - (Retention of knowledge is a <u>skill</u>)
- Intuition is always a response to something
  - Everything it communicates to you is meaningful (although it may occasionally send out a signal that is less than urgent)
- Intuition is a cornerstone of personal safety & Mission safety

Accident signals

- Every accident gives signals before it becomes an accident
  - Anomalies
  - Words, data, or charts in meetings
  - Weak signals
  - Ephemeral signals
- Small errors accumulate
- Failure set in motion from beginning
- Growing apprehension encourages methods of decision making that make failure even more likely, then inevitable
- Develop sensors to detect signals